
# Certification & Accreditation for Wireless LANs

# Wireless: Requirement or Luxury?

- ***In order to justify wireless or for that matter any technology to solve a problem or fulfill a need, the following changes and needs to be identified/enumerated:***
  - ***Justifications***
  - ***Risks***
  - ***Impacts (from adding and removing wireless)***
  - ***Other requirements***
- ***You can't just use wireless because it is cool or sexy!***

# Justification for Wireless

- ***Need to identify the difference between wired and wireless solutions***
  - ***Identify the need(s)***
  - ***Identify each solution's risks, benefits, and additional requirements***
  - ***The justification must prove that wireless is a better solution than wired or standalone. This includes technology, flexibility of use and fiscally as well.***

# Current Wireless Policy

- ***DoD Directive 8100.2 is "High Level"***
  - ***Just released and not intended as Engineering Specifications***
- ***US Navy***
  - ***SECNAV Instruction is in Draft***
  - ***NETWARCOM Instruction is also in Draft***
  - ***NETWARCOM's desire is to release a "Layer 2" solution as part of their policy***
  - ***Since there is no official Navy policy to date, a Moratorium has been released from NNWC and waivers must be requested***
- ***Commercial***
  - ***802.11i is supposed to be released soon and will provide additional guidance***

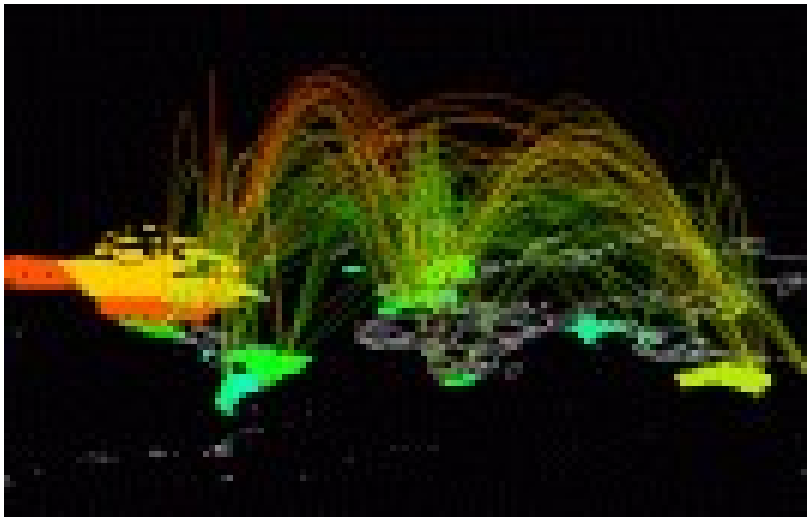
# Wireless Risks

- *C&A revolves around acceptance of Risk. No system is risk free, therefore it is up to the DAA to evaluate the risk and make a informed decision.*

- *Risk = Threat * Vulnerability*
- *A vulnerability is an exploitable feature of an asset.*
- *A threat is the ability of someone to exploit that vulnerability.*
- *Risk is the likelihood that the vulnerability will be exploited.*

# Wireless Risks (cont. 1)

- ***All of the solution's assets, threats, vulnerabilities and risks (****not just the wireless ones****) must be identified.***
- ***Basic Risk Management***
  - ***Acceptance***
  - ***Avoidance***
  - ***Reduction***
  - ***Transference***



# Wireless Risk (cont. 2)

***Describe how you will manage the risk:***

- *Acceptance* **– *Self-explanatory***
- *Avoidance* **– *Remove the technology***
- *Reduction* **– *Alter the threat or vulnerability***
- *Transference* **- *Outsource (not a risk management option for military networks)***

# Wireless Risk (cont. 3)

- ***Use of wireless add risks such denial of service attacks at Layers 1 and 2***
- ***Vulnerabilities in Layer 1 and 2 can be exploited to introduce or exploit vulnerabilities in higher levels of the OSI model (e.g., ARP manipulation can lead to Man-in-the-middle attacks)***

# Wireless Risk (cont. 4)

- ***DOS is crucial because wireless (802.11) technology swaps out Ethernet (802.3) technologies at Layer 1 and parts of Layer 2 (OSI model) provide a transparent solution (e.g. CMSA/CD vs. CMSA/CA).***

- ***Different protocols lead to different risks and different mitigations. They need to be identified.***

# Wireless C&A - DITSCAP

- ***Once you've done all of the above, you need to objectively decide whether or not that wireless connection is absolutely necessary for your mission***

- ***If so, your C&A package must be able to convince the DAA of same and then start working on the SSAA.***

# C&A Primer

- ***The official instruction for DoD C&A is DoDI 5200.40 with the manual being DoD 8510.1-M.***
- ***Entitled the "Department of Defense Information Technology Security Certification & Accreditation Process", these procedures are highly tailorable for all commands, systems, networks and applications.***
- ***DITSCAP is a policy that ensures the leadership, in this case the Designated Approval Authority (DAA), is aware of the risks involved in introducing a new system to the network.***
- ***The result of DITSCAP is an System Security Authorization Agreement or SSAA.***

# SSAA Characteristics

1. Describes the operating environment and threat.
2. Describes the system security architecture.
3. Establishes the C&A boundary of the system to be accredited.
4. Documents the formal agreement among the DAA(s), Certifier, user representative, and program manager.
5. Documents all requirements necessary for accreditation.
6. Documents all security criteria for use throughout the IS life cycle.
7. Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations, architecture description, etc.).
8. Documents the DITSCAP plan.
9. Documents test plans and procedures, certification results, and residual risk.
10. Forms the baseline security configuration document.

**DITSCAP has four phases. The first is the Definition phase and consists of three tasks – Preparation, Registration and Negotiation.**

# Phase I - Preparation Tasks

1. Business Case
2. Mission Needs Statement
3. System Specifications
4. Architecture and Design Documents
5. User Manuals
6. Operating Procedures
7. Network Diagrams
8. Configuration Management Documents
9. Threat Analysis
10. Federal and Organizational IA and Security Instructions and Policies

# Registration

1. Prepare business or operational functional description and system identification.
2. Inform the DAA, Certifier, and user representative that the system will require C&A support (register the system).
3. Prepare the environment and threat description.
4. Prepare system architecture description and describe the C&A boundary.
5. Determine the system security requirements.
6. Tailor the DITSCAP tasks, determine the C&A level of effort, and prepare a DITSCAP plan.
7. Identify organizations that will be involved in the C&A and identify resources required.
8. Develop the draft SSAA.

# Negotiation

1. Conduct the Certification Requirements Review (CRR).

2. Agree on the security requirements, level of effort, and schedule.

3. Approve final Phase 1 SSAA.

# SSAA Tasks & Deliverables by Phase

## Phase I

-System / Func. Descr. & ID
-Register System
-Describe Environ. & Threat
-Determine Sys. Sec. Reqts.
-Describe Sys. Arch
-ID C&A Orgs. & Resources
-Tailor DITSCAP / Write Plan
-Review Cert. Reqts.
-Determine Level of Effort & Schedule
-Basic SSAA

***Appendices:***

A- Acronyms
B- Definitions
C- References
D- CONOPS
E- IS Security Policy
F- Security Requirements and/or Traceability Matrix

## Phase II

- Sys Arch Analysis
- SW / HW Design Analysis
- Network Connection Rule Compliance Analysis
- Integrity Analysis of Integrated Products
- Life-cycle Mgmt Analysis
- Security Rqts. Validation
- CT&E (Type Accred. Only)

***Appendices:***

G- CT&E Plan (Type only)
H- ST&E Plan
K- Incident Resp. Plan
L- Contingency Plans
P- Test & Eval Reports
Q- Prelim Risk Assessment

## Phase III

- ST&E Penetration Testing
- Tempest / Red-Black Verification
- COMSEC Compliance
- System Mgmt Analysis
- Site Accreditation Survey
- Contingency Plan Analysis
- Risk Mgmt Review

***Appendices:***

P- Test & Eval Reports
Q- Residual Risk Assessment

**DoD 8510.1-M**

# Impact of C&A on Wireless LANs

- *When introducing a wireless solution, just like any other new network or system, one needs to individually identify and explain the impact that solution has to other networks, services, and processes.*

- *An example of this would be how wireless technologies interfere with, or can be affected by, other technologies.*

# Wireless Impact (cont. 1)

- *You also need to identify the impact to your organization if you suddenly lose wireless (due to INFOCON, DoS attack, etc.)*

- *Alternatives (contingency plans) must be identified ahead of time and users must be aware of them.*

# Other Rqmts for Wireless C&A

- *External certifications (HERO, HERF, TEMPEST, etc.)*
- *Training (User/SysAdmin/IDS Admin)*
- *Out-of-band management*
- *Wireless IDS*
- *Remote client configuration/management (anti-virus, firewall, patches/updates, account management, etc.)*

# Other Requirements (cont. 1)

- *Periodic Testing (internal/external scans, penetration testing, policy compliance, etc.)*
- *Changes to Incident Reporting/Response Requirements*
- *Configuration requirements inherent to wireless*
- *Users "Acceptable Use" Agreements gains a few new requirements (who, what, when, where and how)*
- *File system encryption for mobile clients*

# WLAN C&A - Conclusion

- ***Like any DoD system, WLANs fall under DITSCAP***
- ***Today there is a moratorium on WLANs from NNWC and waivers must be requested***
- ***New policy is forthcoming and may add additional requirements to WLANs***
- ***There are additional risks inherent with WLANs that must be addressed before implementation.***